

UNITED STATES DISTRICT COURT

JUL 28 2021

for the
Western District of Virginia

JULIA C. DUDLEY, CLERK

BY: 

DEPUTY CLERK

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)Information associated with Google account ID
mrbelman86@gmail.com that is stored at premises
controlled by Google

Case No.

1:21mj 104

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 1951Offense Description
Conspiracy to Interfere with Commerce by Threats or Violence (Hobbs Act robbery)

The application is based on these facts:

See Attached Affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Peter Gonzalves, Special Agent

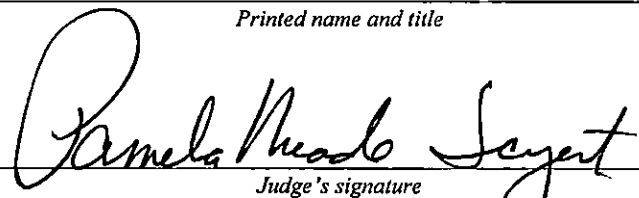
Printed name and title

Sworn to before me and signed in my presence.

Date:

7/28/21

City and state: Abingdon, VA



Judge's signature

Honorable Pamela Meade Sargent, USMJ

Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
ABINGDON DIVISION**

**IN THE MATTER OF THE
SEARCH OF INFORMATION
ASSOCIATED WITH
MRBELTMAN86@GMAIL.COM
THAT IS STORED AT PREMISES
CONTROLLED BY GOOGLE**

Case No. _____

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH
WARRANT**

I, Peter Gonzalves, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with mrbeltman86@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google LLC (hereafter "Google"), an email and cloud storage provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google to disclose to the government records and other information (including the content of communications) in its possession, pertaining to the subscriber or customer associated with the user mrbeltman86@gmail.com.

2. I am an investigative law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18 United States Code, and am empowered by law to conduct investigations and to make arrests for the offenses enumerated in Section 2516 of Title 18 United States Code.

3. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and have been so employed since August 2016. I am currently assigned to the Bristol, Virginia Field Office. Prior to becoming an ATF Special Agent, I was a Special Agent with the U.S. Department of State, Diplomatic Security Service for approximately six years. I have taken part in numerous federal, state, and local investigations concerning document and identity fraud, financial fraud, cybercrimes, and firearms and narcotics violations.

4. During my tenure in law enforcement, I have become familiar with the methods and techniques associated with the distribution of narcotics, the laundering of drug proceeds and the organization of drug conspiracies, and methods and techniques commonly employed during the commission of violent crimes, including robbery. In the course of conducting these investigations, I have been involved in the use of the following investigative techniques: interviewing confidential sources and cooperating witnesses; conducting physical surveillance; controlled buys; consensual monitoring and recording of both telephonic and non-telephonic communications; analyzing telephone pen-register data; requesting,

collecting and analyzing billing records; and conducting court-authorized electronic surveillance. Further, I have participated in the preparation, presentation and execution of numerous search and arrest warrants which have resulted in the recovery of weapons, narcotics, money, and documentary evidence indicative of firearm and narcotic trafficking organizations. Additionally, I have assisted in investigations and arrests leading to convictions for violations of federal and state firearms and narcotics laws to include violent crime.

5. Through instruction and participation in investigations, I have become familiar with the manner and methods by which narcotics traffickers and perpetrators of violent crimes conduct their illegal business and the language and terms that are used to disguise conversations about their illegal activities. From experience and training, I have learned, among other things, that in conversations narcotics traffickers and violent criminals believe susceptible to interception, they virtually never expressly refer to the illegal drugs or weapons or crimes by name; instead to conceal the true nature of their illegal activities and to thwart detection by law enforcement, they refer to the drugs, drug quantities, crimes, and weapons using seemingly innocent terms. I am also aware that violent crime conspiracies are often hatched in advance of the event, and often involve electronic communications between coconspirators and others before and after the crime is perpetrated. These communications often show planning and post-crime

discussions.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

7. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the Google account mrbeltman86@gmail.com, described in Attachment A, contains electronically stored information, as described in Attachment B, consisting of evidence, instrumentalities, contraband, and/or fruits of violations by Michael MILLER and others of 18 U.S.C. § 1951, Conspiracy to Interfere with Commerce by Threats or Violence (Hobbs Act robbery). There is also probable cause to search the information described in Attachment A for evidence of this crime and contraband or fruits of this crime, as described in Attachment B.

PROBABLE CAUSE

8. On May 9, 2021, at approximately 8:15 PM, an individual entered Bare's Discount Tobacco and Wine ("Bare's") located at 970 E. Main St. in Abingdon, Virginia, which is located in Washington County in the Western Judicial District of Virginia. According to the store clerk (hereafter known as

“Victim 1”) who was on duty at the business at the time, the individual produced a handgun and demanded access to the cash register and money safes. Victim 1 described the suspect as a tall and muscular white male, wearing a knit hat, a bandana covering his face, blue jeans, and a green jacket. The clerk also reported the suspect placed a black handgun on the counter as he demanded cash. At approximately 8:23 PM, the suspect exited the store after taking approximately \$35 in cash and two cartons of cigarettes without paying. Other than Victim 1 and the suspect, no additional individuals can be seen on security footage in the store during the time the suspect was inside the business.

9. Bare’s sells alcohol, tobacco and packaged food products, many of which were manufactured and/or procured from sources outside the state of Virginia and therefore moved in interstate commerce.

10. Investigators with the Abingdon, Virginia Police Department (APD) later reviewed surveillance footage provided by Bare’s and other businesses in the surrounding area. Surveillance footage shows that, at approximately 7:30 PM on May 9 (surveillance footage timestamp), a white Dodge Journey with an unknown license plate (hereafter referred to as “the suspect vehicle”) drove around the exterior of Bare’s and the adjacent businesses. The suspect vehicle also drove in circles through the parking lots of other businesses in the immediate vicinity.

11. From approximately 8:07 PM through 8:12 PM, the suspect vehicle drove through parking lots of businesses between the BP station located at 906 E. Main St. in Abingdon, Virginia and Bare's. At approximately 8:20 PM, the suspect vehicle can be seen pulling into the BP gas station parking lot. An employee at the BP reported seeing a white Dodge Journey in the parking lot occupied by two individuals, and that one of the individuals exited the vehicle behind the BP station. At approximately 8:20 PM, an individual wearing similar clothing and matching the physical description of the suspect can be seen walking from the rear of the BP parking lot in the direction of Bare's. At approximately 8:15 PM, the suspect entered Bare's and encountered Victim 1. At approximately 8:23 PM, the suspect exited the store and can be seen on surveillance footage walking from the area of Bare's toward the BP station.

12. On or about May 11, 2021, an investigator with the Washington County Sheriff's Office (WCSO) reported having a phone conversation with Michael MILLER after the robbery occurred. During this conversation, MILLER informed the investigator he was driving a white Dodge Journey belonging to "B.H." during the previous weekend. B.H. is an associate of MILLER's, though there is no evidence to date of B.H. participating in the conspiracy. The WCSO investigator provided two telephone numbers from which WCSO has received calls from

MILLER in the weeks and months prior to the robbery: 276-608-7196 and 540-835-3859.

13. On or about May 23, 2021, Verizon produced certain subscriber and device information associated with these two phone numbers. The International Mobile Equipment Identifier (IMEI) associated with 276-608-7196 from March 15, 2021, through May 20, 2021, is 352082504971013. The IMEI associated with 540-835-3859 from April 30, 2021, through May 20, 2021 is 357754083696972. An IMEI is akin to a unique electronic serial number and identifies a particular device on a cellular network. Verizon's records also indicated the device model associated with 276-608-7196 is a Samsung SM-S111DL. Publicly available information on the internet indicates this device runs Android as its operating system, which is produced and supported by Google. Please see the next section in this affidavit for additional information regarding Google and Android.

14. On June 30, 2021, deputies with the WCSO arrested MILLER on outstanding state arrest warrants from other jurisdictions. During a post-*Miranda* interview, MILLER stated he and Robert DAWSON were together in B.H.'s vehicle on the day of the robbery. MILLER stated that while driving around, DAWSON asked MILLER to drop him off at the BP gas station for an unknown reason. MILLER later stated he and DAWSON discussed how easy it would be to rob Bare's, but MILLER indicated the conversation between him and DAWSON was

meant in jest and that he did not actually intend to rob the store. MILLER further stated this conversation took place at Bare's in the afternoon on the day of the robbery, and DAWSON and Victim 1 were both present. MILLER also stated to investigators that Victim 1 is a "dear friend."

15. On June 30, 2021, investigators interviewed Victim 1. Victim 1 stated he/she observed a tall, muscular individual enter the store. After picking up a drink from the cooler, the individual approached the counter, demanded money from the register, and placed a small handgun on the counter. Victim 1 was unable to determine if it was a real firearm, but described it as small, black, and "old" looking. Victim 1 stated that he/she debated with the individual for several minutes and did not want to open the register for the suspect. Victim 1 stepped out from behind the counter, and the suspect attempted to open the cash register unsuccessfully. The suspect then took approximately \$35 in cash from a lockbox and two cartons of cigarettes, both of which were located behind the counter, before leaving the store.

16. Victim 1 also admitted to having a relationship with MILLER. Victim 1 stated that he/she was initially hesitant to disclose that fact as Victim 1 is presently married. Victim 1 further stated that he/she was with MILLER at B.H.'s residence the day after the robbery. Victim 1 also stated the other individual who was with MILLER and Victim 1 at Bare's the day of the robbery was also present. Based on MILLER's and Victim 1's statements, investigators concluded the second male

present at B.H.'s residence at that time was DAWSON. That evening, Victim 1 overheard MILLER and DAWSON talking about the robbery. According to Victim 1, MILLER and DAWSON were upset about only getting \$35 and two cartons of cigarettes. Victim 1 also stated that MILLER said he dropped DAWSON off and picked him up again after the robbery.

17. On or about July 1, 2021, Google produced records in response to a subpoena concerning account information linked to IMEIs 352082504971013 and 357754083696972. Google's records indicated the Google account that was attached to IMEI 352082504971013 (associated with 276-608-7196, according to Verizon) from April 1, 2021, through June 29, 2021 is mrbeltman86@gmail.com. The name listed in subscriber information for that account is Mike Miller. Google did not find records associated with IMEI 357754083696972 (associated with 540-835-3859, according to Verizon).

18. Google also produced subscriber information and certain records pertaining to the Google Pay service linked with the mrbeltman86@gmail.com account. Among other details, customers typically provide their name, address, and phone number when setting up a Google Pay account. Customer-provided information collected by Google for this account shows the customer name as Mike Miller, and customer phone number as 540-835-3859. This matches a phone number used by MILLER on previous occasions to contact WCSO. While

this number matches a number known to be used by MILLER around the time of the robbery, it appears in this context in customer-provided information collected by Google. Its appearance in the Google Pay records for the mrbeltman86@gmail.com account is unrelated to phone records or IMEI information provided by Verizon.

19. Google records also indicated there was a different account associated with the phone number 276-608-7196. However, neither of the IMEI numbers connected with MILLER's phone numbers appear to be connected with that different account.

20. Based on my training and experience, I know most people commonly carry at least one mobile device with them when outside their residence. Whether actually on their person or close at hand, the vast majority of people keep their mobile devices within close proximity wherever they go. This leads to a high probability that if law enforcement identifies the location of an individual's mobile device, the owner will be close by. I am also aware that violent crime conspiracies are often hatched in advance of the event, and often involve electronic communications between coconspirators and others before and after the crime is perpetrated. These communications often show planning and post-crime discussions, and are often conducted both in-person and utilizing messaging services on mobile devices. These communications often remain on providers'

servers, on the involved mobile devices themselves, or both. Based on my training experience, I believe it is likely that, on the day of the robbery described above, MILLER was carrying the device associated with phone number 276-608-7196 and IMEI 352082504971013.

BACKGROUND CONCERNING GOOGLE

21. Based upon my training and experience and information acquired from other law enforcement officials with technical expertise, I have learned the following information. Google provides a variety of online services to the public, including electronic mail ("email"). Google allows subscribers to obtain email accounts at the domain name gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Google maintains information about the mobile devices associated with the subscribers' Google accounts. This includes the make, model, and unique serial numbers of all linked devices. Google also maintains information about its subscribers, including primary email addresses, secondary email addresses for account password recovery, applications, websites, and services that are allowed to access the subscribers' Google accounts or use the subscribers' Google accounts as a password login, and account login activity such as the geographic area in which a subscriber logged into their account, what type of internet browser and/or

device the subscriber was using, and the internet protocol (IP) address from which they logged in. The IP address is roughly analogous to a telephone number assigned to a computer by an internet service provider. The IP address can be resolved back to a physical address, such as a residence or business with Wi-Fi access or residential cable internet. I believe this information will assist in the investigation by identifying previously unknown email accounts and devices utilized by the suspect, as well as location history information tending to show the movements of the suspect and his/her mobile device(s).

22. Google subscribers can enroll Android devices with an associated Google account into a device backup service. This backup service duplicates some of the information stored on the device in the event the user loses his or her device or it becomes otherwise inoperable. Device backup data is limited to data from applications stored on the device, all history including dialed, received, and missed calls, and device settings. The backup files are named with the device's manufacturer and model number in the user's Google Drive service.

23. A Google subscriber can also store with the provider other files in addition to emails, such as address books, favorite locations, contact or buddy lists, calendar data, pictures, and videos, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, emails in the account, and

attachments to emails, including pictures and files, as well as in the location history. Based on my training and experience, I believe this information could show the suspect's location at the time the above-mentioned violations were committed.

24. Google Maps is a web service and application that allows users to search for places and routes to navigate using public transportation, vehicle, bicycle, or foot. Users can label or designate specific places in Google such as home or work. Google maps also records commute routes and commute settings based on recorded patterns such as date and time, origin and destination, and route traveled. Based on my training and experience, I believe this information would allow law enforcement to show patterns of travel, which may corroborate or disprove other evidence in this case.

25. Google Pay is an internet-based payment service where customers can enroll credit and debit/bank cards in order to make payments to third parties for goods and services. Users can then use Google Pay as a form of payment to online retailers as a substitute for inputting credit card information on retailers' websites when making purchases. Google Pay also has a companion mobile device application that performs a similar function using the point-of-sale systems at "brick and mortar" retailers. Like any other online service, Google Pay asks customers for certain pieces of information to register accounts. Customers typically provide

name, addresses, telephone numbers and email addresses for their Google Pay accounts in addition to linking payment cards and bank accounts.

26. Chrome is an internet browser developed and distributed by Google. The Chrome browser is tightly integrated with other Google products and is the default browser installed on the Android operating system. The Chrome browser collects and stores information which is transmitted to Google and retained by the company. This information includes autofill and auto-populate data from prior searches, bookmarked webpages, browser history showing searched-for words, extensions, and add-ons that are developed by Google and third parties to bring custom features to the browser, search engines used, and sync settings so the user can have the previously listed features across multiple devices. Based on my training and experience, I believe this information would show the suspect's internet activity during the activity described above.

27. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of crimes under investigation because the information can be used to

identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

28. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of services utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account.

29. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

30. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling law enforcement to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described above, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (*e.g.*, location

information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

31. Searching for the evidence described in this warrant application may require a range of data analysis techniques. In some cases, law enforcement officers and computer analysts may be able to conduct carefully targeted searches to locate evidence without needing to carry out a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Numerous types of user information and metadata stored on a cellphone are not susceptible to "word search" or similar forensic techniques, including but not limited to images, audio and video recordings, and proximate GPS locations. In addition, the complex interrelatedness of cell-phone data may undermine the efficacy of narrow search techniques based on the type, location, or date of information. Indeed, the vast array of applications now available on cellular telephones makes it extremely hard to determine the exact form and organization of user information and metadata prior to conducting a search. Finally, criminals can mislabel, misspell, or

hide information; encode communications to avoid using key words; attempt to delete information to evade detection; or take other steps designed to frustrate law enforcement searches for information.

32. Accordingly, law enforcement officials or other analysts with appropriate expertise may need to conduct more extensive searches not obviously related to the evidence described in this warrant application or perusing all stored information briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, ATF and its partners intend to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in this warrant application.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

33. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

34. Based on the forgoing, I request that the Court issue the proposed search warrant.

35. This Court, the United States District Court for the Western District of Virginia, has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711 and 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A).

36. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

37. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to

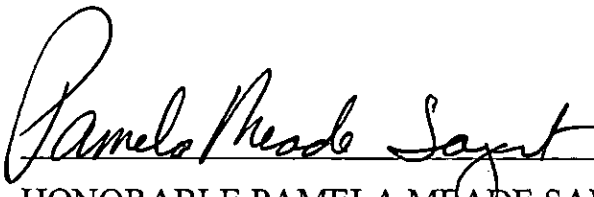
flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,



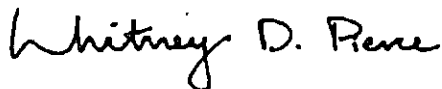
Special Agent Peter Gonzalves
Bureau of Alcohol, Tobacco, Firearms,
and Explosives
United States Department of Justice

Subscribed and sworn to before me on July 28, 2021.



HONORABLE PAMELA MEADE SARGENT
UNITED STATES MAGISTRATE JUDGE

Reviewed by: Whit Pierce, AUSA



ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with mrbeltman86@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to the request made under 18 U.S.C. § 2703(f) on or about June 29, 2021, the Provider is required to disclose the following information to the government for the account or identifier listed in Attachment A:

A. The contents of all emails associated with the account from May 1, 2021, to May 15, 2021, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

B. All records or other information regarding the identification of the account or linked to the account, to include full name, physical address, telephone numbers and other identifiers, any and all data stored as part of the individual's use of the following Google services: 3D Warehouse, AdManager, AdPlanner, AdSense, AdWords, Alerts, Analytics, Apps, Base, Blogger, Bookmarks, Buzz, Calendar, Checkout, Contacts, Dashboard, Docs, Friend Connect, Groups, Health, Merchant Center, Notebook, Orkut, Picasa, Profiles, Reader, Talk, Tasks, Voice, and Wave; records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, device identifiers associated with any device that has logged into this account or device that has been linked to this account, alternative email addresses or phone numbers provided during registration, account recovery methods including any form of contact information provided, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

C. All Backup files, stored in Google Drive or elsewhere, including associated data such as application data call history, device settings, contacts, calendar information, short message system files consisting of data, time, sender, receiver, and message content, photos and videos;

D. Android Information-Device make, model, and International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of all associated devices linked to mrbeltman86@gmail.com;

E. Contacts -- All contacts stored by Google including name, all contact phone numbers, emails, social network links, and images;

F. All Chrome data including autofill, bookmarks, browser history, extensions, dictionary, search engine, and sync settings;

G. Gmail -- All email messages, including by way of example and not limitation, such as inbox messages whether read or unread, sent mail, saved drafts, chat histories, and emails in the trash folder. Such messages will including all information such as the date, time, internet protocol (IP) address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the "cc" (carbon copy) or the "bcc" (blind carbon copy), the message content or body, and all attached files;

H. Google Photos -- All images, graphic files, video files, and other media files stored in the Google Photos service;

I. Google Maps -- All Google Maps data including commute routes, commute settings, and labeled places;

J. Google Location History / Google Timeline data for any devices associated with mrbeltman86@gmail.com to include, but not limited to, all location data whether derived from Global Positioning System (GPS), cell site / cell tower triangulation / multi-alteration, precision measurement information such as timing advance, or per call measurement data, Wi-Fi location, Bluetooth, or device sensors, including accelerometer, barometer, gravity, magnetic field, orientation, or proximity. Such data shall include the GPS coordinates and the dates and times of all location recordings from the period of May 1, 2021, through May 15, 2021;

K. Play Store -- All applications downloaded, installed, and / or purchased by mrbeltman86@gmail.com;

L. Web and Application history -- All search history and queries, including by way of example and not limitation, World Wide Web (web) browsing, images, news, shopping, ads, videos, maps, travel, and finance, whether performed in private browsing, incognito, anonymous or secret mode, all device activity including application use, social media use, device phone

functions such as calling and/or text messaging activity, email activity including read, sent, and received emails, and the dates and times of searches made and applications used;

M. Voice – All call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voicemail messages sent by or from the Google Voice account associated with mrbelzman86@gmail.com;

N. Docs (Documents) – All Google documents including by way of example and not limitation, Docs (a web-based word processing application) and Sheets (a web-based spreadsheet program). Documents will include all files whether created, shared, or downloaded;

O. The types of service utilized;

P. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

Q. All location information pertaining to the account or linked to the account from the time period of May 1, 2021 to May 15, 2021;

R. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities pertaining to violations of the statute listed on the warrant, for the account or identifier listed in Attachment A, including information pertaining to the following matters:

- A. All records or information, including the contents of any and all wire and electronic communications, attachments, header information, or other stored files, that will assist investigators in ascertaining the nature and scope of the crime under investigation; the true identity and/or location of the suspect and any co-conspirators; and any disposition of the proceeds of the crime under investigation; and
- B. Records related to who created, used, or communicated with the account or identifier.